PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-351747
(43)Date of publication of application : 06.12.2002

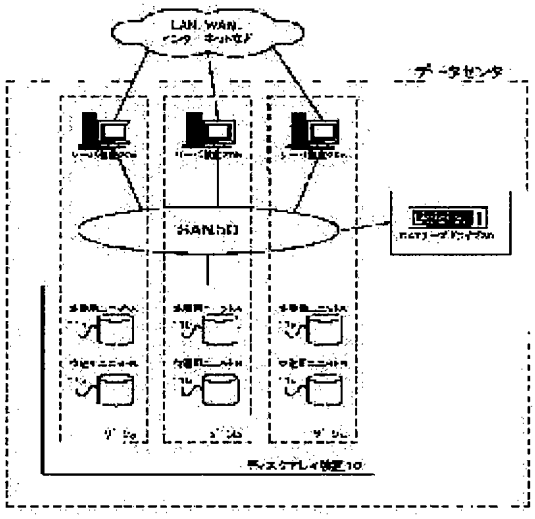
(51)Int.Cl. G06F 12/16
G06F 3/06
G06F 12/00
G06F 12/14

(21)Application number : 2001-163202
(22)Date of filing : 30.05.2001

(71)Applicant : HITACHI LTD
(72)Inventor : SUZUKI HIROYOSHI
TAJI IWAO

(54) BACKUP MANAGING METHOD FOR IN-STORAGE DATA OF STORAGE SYSTEM AND STORAGE SYSTEM EQUIPPED WITH MEANS FOR IMPLEMENTING THE SAME MANAGING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a backup managing method for in-storage data of a storage system which can assure high data security.
SOLUTION: The storage system includes a storage 10 having a plurality of storage areas 11 given access restrictions individually and a removable media type backup device 30. When the data in a certain storage area 11 are backed up, the data are ciphered with a key given uniquely to the storage area 11 and the ciphered data are stored in specified removable media set in a backup device through SAN 50. When the data in the certain storage area 11 are reloaded, the removable media are set in the backup device, the ciphered data stored in the media are transmitted to the storage 10 through the SAN 50, deciphered with the key given to the storage area 11, and stored into the storage area 11.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－351747
（P2002－351747A）
(43)公開日　平成14年12月６日(2002.12.6)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	12/16	３１０	Ｇ０６Ｆ 12/16	３１０Ｍ	５Ｂ０１７
	3/06	３０４	3/06	３０４Ｆ	５Ｂ０１８
	12/00	５３１	12/00	５３１Ｍ	５Ｂ０６５
		５３７		５３７Ｈ	５Ｂ０８２
	12/14	３２０	12/14	３２０Ｂ	

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願2001－163202(P2001－163202)

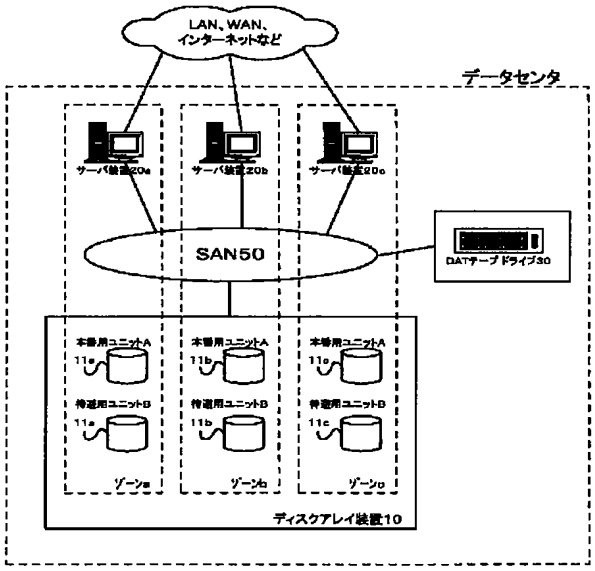
(22)出願日　平成13年５月30日(2001.5.30)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　鈴木　啓悦
神奈川県小田原市中里322番地２号　株式会社日立製作所ＳＡＮソリューション事業部内
(72)発明者　田路　巌
神奈川県小田原市中里322番地２号　株式会社日立製作所ＳＡＮソリューション事業部内
(74)代理人　100071283
弁理士　一色　健輔　（外５名）

最終頁に続く

(54)【発明の名称】　ストレージシステムにおけるストレージ内データのバックアップ管理方法およびこの管理方法を実施する手段を備えたストレージシステム

(57)【要約】
【課題】　高いデータセキュリティを確保することができる、ストレージシステムにおけるストレージ内データのバックアップ管理方法を提供する。
【解決手段】　個別にアクセス制限が施された複数の記憶エリア１１を有するストレージ１０とリムーバブルメディア方式のバックアップ装置３０とを含むストレージシステムにおいて、ある記憶エリア１１のデータのバックアップに際してはその記憶エリア１１に固有に付与したキーにより暗号化してその暗号化データをバックアップ装置にセットされている所定のリムーバブルメディアにＳＡＮ５０を通じて格納し、ある記憶エリア１１のデータの復旧に際しては該当のリムーバブルメディアをバックアップ装置にセットしてこれに格納されている暗号化データをＳＡＮ５０を通じてストレージ１０に伝送しこれを前記記憶エリア１１に付与されたキーにより復号化して前記記憶エリア１１に格納する。



1

【特許請求の範囲】

【請求項１】　個別にアクセス制限が施された複数の記憶エリアを有するストレージとこのストレージにアクセスするサーバ装置とリムーバブルメディア方式のバックアップ装置とが所定の通信手段によりネットワーク接続されているストレージシステムにおけるストレージ内データのバックアップ管理方法であって、

前記記憶エリアのうちのある記憶エリアＡのデータのバックアップに際しては記憶エリアＡのデータを記憶エリアＡに固有に付与したキーにより暗号化した暗号化データを前記通信ネットワークを通じて前記バックアップ装置にセットされている所定のリムーバブルメディアに格納し、

記憶エリアＡのデータの復旧に際しては該当のリムーバブルメディアを前記バックアップ装置にセットしてこれに格納されている暗号化データを前記通信ネットワークを通じて前記ストレージに伝送し、これを記憶エリアＡに付与された前記キーにより復号化して記憶エリアＡに格納することを特徴とする。

【請求項２】　請求項１に記載のストレージシステムにおけるストレージ内データのバックアップ管理方法であって、

前記所定の通信手段がＳＡＮであり、

前記記憶エリアが一台もしくは複数台のハードディスクユニットにより提供され、

前記ハードディスクユニットのうちのあるハードディスクユニットＡのデータをそのハードディスクユニットに固有に付与したキーにより暗号化してこの暗号化データをハードディスクユニットＡとは別の前記ハードディスクユニットに記憶管理し、

ハードディスクユニットＡのデータのバックアップに際しては前記暗号化データを前記ＳＡＮを通じて前記バックアップ装置にセットされている所定のリムーバブルメディアに格納し、

ハードディスクユニットＡのデータの復旧に際しては該当のリムーバブルメディアを前記バックアップ装置にセットしてこれに格納されている暗号化データを前記ＳＡＮを通じて前記ストレージに伝送しこれをハードディスクユニットＡに付与された前記キーにより復号化してハードディスクユニットＡに格納するようにすることを特徴とする。

【請求項３】　請求項２に記載のストレージシステムにおけるストレージ内データのバックアップ管理方法であって、前記アクセス制限が前記ＳＡＮのゾーニング機能もしくはマスキング機能により設定されたものであることを特徴とする。

【請求項４】　請求項２に記載のストレージシステムにおけるストレージ内データのバックアップ管理方法であって、前記暗号化データを前記ハードディスクユニットＡに格納されているデータの変更に応じてリアルタイムに生成し、前記暗号化データを前記ハードディスクユニットＡとは別の前記ハードディスクユニットに同時並行的に記憶管理することを特徴とする。

2

【請求項５】　請求項１～４のいずれかに記載のバックアップ管理方法を実施する手段を備えたストレージシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ストレージシステムにおけるストレージ内データのバックアップ管理方法に関し、とくにリムーバブルメディア方式のバックアップ装置を利用してストレージ内データを集中的にバックアップ管理する際におけるデータセキュリティを確保するための技術に関する。

【０００２】

【従来の技術】ＡＳＰ市場の拡大、企業システムのアウトソーシング指向に伴い、データセンタの需要が増大している。典型的なデータセンタにおけるストレージシステムの概略構成を図６に示す。ディスクアレイ装置などのストレージ１０と、ＬＡＮやＷＡＮ、インターネットなどを通じてデータセンタ外の機器に接続しこれらとストレージ１０との間に介在するサーバ装置２０ａ，２０ｂ，２０ｃと、ストレージ１０内のデータをバックアップするバックアップ装置３０（ＤＡＴテープドライブ）とがＳＡＮ（Storage Area Network）５０により接続されている。

【０００３】ところで、データセンタにおいては、データの一括管理によるスケーラブルメリットを最大限に生かすため、一台のストレージ１０に異なるシステムや異なるユーザのデータを混在させて運用管理するのが一般的である。そのため、データセンタでは、通常、ストレージ１０内に実装されたハードディスクユニットなどの各記憶資源について、ゾーニングやマスキングなどの機能を用いてシステムごと或いはユーザコンピュータごとのアクセス制限を施すことで、データセキュリティの確保を図っている。

【０００４】一方、データセンタではディスククラッシュなどのトラブルに対する危機管理も重要であり、通常、データセンタではＳＡＮ５０の特徴を生かしたＬＡＮフリー・バックアップやサーバ・フリー・バックアップといった手法を用いてＳＡＮ５０に接続されたバックアップ装置３０により集中的なバックアップ管理を行っている。なお、前記のバックアップ装置３０としては、ビット単価の比較的安価なＤＡＴテープドライブなどのリムーバブルメディア方式のものが採用されることが多く、バックアップ装置３０にはリムーバブルメディアの脱着を行うためのオペレータが配置されるのが普通である。

【０００５】

【発明が解決しようとする課題】ところで、前記のリム

ーバブルメディアの脱着に際しては、オペレータには細心の注意が要求される。何故なら、万が一、指定されたメディアと異なるメディアを間違えてバックアップ装置３０にセットしてしまった場合には、あるシステムやユーザ用にアクセス制限された記憶資源に他のシステムやユーザのデータが格納されてしまうこととなり、データセンタの信用にかかわる重大な事故につながるおそれがあるからである。

【０００６】しかしながら、オペレータも人間であるからこのような人為的なミスを完全に防ぐことは難しく、従って、このような事故を未然に防ぐ仕組みを設けることがデータセンタの運用上好ましい。

【０００７】本発明はこのような観点からなされたものであって、高いデータセキュリティを確保することができる、ストレージシステムにおけるストレージ内データのバックアップ管理方法およびこの管理方法を実施する手段を備えたストレージシステムを提供することを目的とする。

【０００８】

【課題を解決するための手段】この目的を達成するための、本発明の主たる発明は、個別にアクセス制限が施された複数の記憶エリアを有するストレージとこのストレージにアクセスするサーバ装置とリムーバブルメディア方式のバックアップ装置とが所定の通信手段によりネットワーク接続されているストレージシステムにおけるストレージ内データのバックアップ管理方法であって、前記記憶エリアのうちのある記憶エリアＡのデータのバックアップに際しては記憶エリアＡのデータを記憶エリアＡに固有に付与したキーにより暗号化した暗号化データを前記通信ネットワークを通じて前記バックアップ装置にセットされている所定のリムーバブルメディアに格納し、記憶エリアＡのデータの復旧に際しては該当のリムーバブルメディアを前記バックアップ装置にセットしてこれに格納されている暗号化データを前記通信ネットワークを通じて前記ストレージに伝送し、これを記憶エリアＡに付与された前記キーにより復号化して記憶エリアＡに格納するようにしたものである。

【０００９】

【発明の実施の形態】図１に本発明の一実施例として説明する、データセンタに設置されたストレージシステムの概略構成を示している。ファイバチャネルストレージとして機能するディスクアレイ装置１０と、ＬＡＮやＷＡＮもしくはインターネットなどの外部ネットワークを介してこのデータセンタの利用者である企業などのコンピュータに接続しこれらとディスクアレイ装置１０との間に介在するサーバ装置２０と、ＤＡＴテープドライブ３０とが、ファイバチャネルスイッチやファイバチャネルブリッジなどのネットワークデバイスで構成されたＳＡＮ５０に接続され、ストレージシステムを構成している。

【００１０】図２はディスクアレイ装置１０の概略構成である。複数台のハードディスクユニット１１が実装され、これら制御するドライブ制御部１２、ＳＡＮ５０との間の接続を制御するチャネル制御部１３、共用メモリ１４やキャッシュメモリ１５、ディスクアレイ装置１０内の各種制御や稼働状況監視、障害検知および各種情報管理（例えば、実装されているハードディスクユニット１１の物理シリンダ数やアクセス頻度などの管理）などを行うサービスプロセッサ１６などを備えている。

【００１１】ハードディスクユニット１１には、ファイバチャネルスイッチおよびディスクアレイ装置などが備えるゾーニングやマスキングなどの機能によってアクセス制限が施されている。例えば、図１の場合では、ハードディスクユニット１１ａ、１１ｂ、１１ｃにそれぞれ個別にアクセス制限（ゾーンａ、ｂ、ｃ）が施され、ハードディスクユニット１１ａ、１１ｂ、１１ｃはそれぞれ独立した記憶エリアを構成しており、例えば、サーバ装置２０ａはゾーンａのハードディスクユニット１１ａにはアクセスできるが、ゾーンｂのハードディスクユニット１１ｂやゾーンｃのハードディスクユニット１１ｃにはアクセスすることはできない。

【００１２】ディスクアレイ装置１０のハードディスクユニット１１の一部は、サーバ装置２０ａからの直接的な読み出しや書き込みが可能な本番用ユニットＡに割り当てられ、また、他の一部は本番用ユニットＡのバックアップデータを格納するための待避用ユニットＢに割り当てられている。各本番用ユニットＡと待避用ユニットＢとの対応づけは、システム管理者などがディスクアレイ装置１０の管理端末などから手動で設定する方法、サービスプロセッサ１６が、例えば、各ハードディスクユニット１１が実装されているスロットの位置を自動認識して設定する方法などの各種の方法により設定される。ディスクアレイ装置１０は、この本番用ユニットＡと待避用ユニットＢとの対応付けを、各ハードディスクユニット１１に付与された固有のユニットＩＤにより図３に示す管理テーブルに記憶管理している。

【００１３】待避用ユニットＢに格納されるバックアップデータは、本番用ユニットＡのデータそのものでなく、これを暗号化したものである。ディスクアレイ装置１０は、各本番用ユニットＡのデータをリアルタイムに暗号化し、各本番用ユニットＡに対応づけられている待避用ユニットＢにリアルタイムに格納する。これにより待避用ユニットＢには、本番用ユニットＡのデータの暗号化データが同時並行的に記憶管理される。

【００１４】暗号化は、各本番用ユニットＡとこれに対応づけられた待避用ユニットＢのペアごとに固有に設定されたキーを用いて行われる。キーは、ディスクアレイ装置１０により自動的に生成される場合、システム管理者などにより手動で設定される場合など、様々な方法で設定される。キーは、本番用ユニットＡと待避用ユニッ

トＢの組み合わせに対応づけて前記管理テーブルに記憶管理される。

【００１５】ところで、この実施例で説明するストレージシステムでは、本番用ユニットＡのデータのバックアップに際し本番用ユニットＡのデータをそのままバックアップするのではなく、これに対応づけられている待避用ユニットＢに格納されている暗号化データの方をバックアップするようにしている。これはバックアップに関する一連の処理が本番用ユニットＡに与える負荷を極力抑え、本番用ユニットＡを利用している各種システムやユーザへの影響を減らすためである。

【００１６】バックアップはつぎの手順で行われる。まず、ディスクアレイ装置１０は、ＳＡＮ５０を通じてＤＡＴテープドライブ３０にＤＡＴテープのセット指示を送信する。これによりＤＡＴテープドライブ３０は、付属の管理用ディスプレイにＤＡＴテープをセットするよう表示する。ここでこの指示には、バックアップ対象となる本番用ユニットＡを特定するユニットＩＤが含まれ、管理用ディスプレイには前記セット指示に付帯してユニットＩＤも表示される。オペレータは、これらの表示を確認すると、該当の本番用ユニットＡ用に用意されたＤＡＴテープを管理ラックから探し出してＤＡＴテープドライブ３０にセットする。

【００１７】つぎに、ＤＡＴテープが正常にセットされると、その旨がＳＡＮ５０を通じてディスクアレイ装置１０に通知され、バックアップ対象となる本番用ユニットＡに対応する待避用ユニットＢに格納されている暗号化データが、ＳＡＮ５０通じてディスクアレイ装置１０からＤＡＴテープドライブ３０に伝送されて、前記ＤＡＴテープに前記暗号化データが格納される。暗号化データのＤＡＴテープへの格納が完了すると、管理用ディスプレイにその旨が表示される。これを見たオペレータはＤＡＴテープをＤＡＴテープドライブ３０から取り外し、そのＤＡＴテープを管理用ラックの所定位置に収納する。

【００１８】一方、ＤＡＴテープにバックアップされた暗号化データは、例えば、ディスククラッシュなどにより本番用ユニットＡのデータが紛失等した場合のデータの復旧処理に利用される。つぎに、この復旧処理の手順を図４に示すフローチャートとともに説明する。

【００１９】ディスクアレイ装置１０は、ある本番用ユニットＡに何らかの異常が発生し、ＤＡＴテープにバックアップされた暗号化データを利用する必要があると判断すると、ＤＡＴテープドライブ３０にその本番用ユニットＡに対応する暗号化データ（すなわち、この本番用ユニットＡに対応する待避用ユニットＢからバックアップした暗号化データ）が格納されているＤＡＴテープのセット指示を、ＳＡＮ５０を通じて送信する（１１０）。ＤＡＴテープドライブ３０は、このセット指示を受信すると、その旨およびこのセット要求通知に付帯する前記本番用ユニットＡのユニットＩＤを、管理用ディスプレイに表示する（１２０）。オペレータは、このセット指示を確認すると、該当のＤＡＴテープを管理ラックから探し出し、そのテープをＤＡＴテープドライブにセットする（１３０）。

【００２０】ＤＡＴテープが正常にセットされると、つぎに、その旨がＳＡＮ５０を通じてディスクアレイ装置１０に通知され、ＤＡＴテープドライブ３０にセットされているＤＡＴテープに格納されている暗号化データが、ディスクアレイ装置１０に伝送される。ディスクアレイ装置１０は、伝送されてきた暗号化データを、前記本番用ユニットＡに対応づけられている待避用ユニットＢに格納する（１４０）。

【００２１】以上により暗号化データが待避用ユニットＢに格納されると、つぎに、ディスクアレイ装置１０は管理テーブルを参照し、前記本番用ユニットＡに対応づけられているキーにより待避用ユニットＢに記憶されている暗号化データの復号化を試みる（１５０）。ここでこのキーが待避用ユニットＢに格納されている暗号化データの暗号化の際に使用したキーと一致する場合には、正常に復号化が行われ、ディスクアレイ装置１０は復号化されたデータを前記本番用ユニットＡに格納し、これにより前記本番用ユニットＡのデータ復旧処理が無事完了する（１６０）。

【００２２】他方、キーが不一致の場合には、復号化を行うことができず、この場合、ディスクアレイ装置１０は、当該装置１０の管理端末のディスプレイなどにその旨を通知するエラーメッセージを表示する（１７０）。そして、これを見て復号化ができなかったことを知ったシステム管理者は、ＤＡＴテープの掛け間違えたかどうかをオペレータに確認し、掛け間違えであった場合には、オペレータに正しいＤＡＴテープをＤＡＴテープドライブ３０にセットし直してもらうなどの対応を講じることとなる。

【００２３】以上に説明したように、本発明によれば、万が一、オペレータがＤＡＴテープを掛け間違えてセットしても、あるシステムやユーザにアクセスが許可されたハードディスクユニットに他のシステムやユーザの暗号化データが格納されてもキーが一致しない以上その暗号化データが復号化されることはなく、高いデータセキュリティが確保されることになる。また、万が一、ＤＡＴテープが盗まれても、キーが知られない以上、元のデータを復元することはできず、この点でもデータセキュリティが確保されることになる。

【００２４】ところで、以上の実施例は、待避用ユニットＢに格納されている暗号化データをバックアップする構成であったが、例えば、本番用ユニットＡのデータをディスクアレイ装置１０が直接暗号化し、この暗号化データを直接ＳＡＮ５０を通じてＤＡＴテープドライブ３０に伝送してリムーバブルメディアにバックアップし、

データ復旧時には該当のＤＡＴテープに格納されている暗号化データをＤＡＴテープドライブからＳＡＮ５０通じてディスクアレイ装置１０に伝送して復号化する、といった構成も考えられる。なお、この方式を採用した場合には、図１に示すように各ゾーンに必ずしも複数のハードディスクユニットが含まれている必要はなく、一つのゾーンに一台のハードディスクユニットしか含まれなくてもよいことになる。

【００２５】アクセス制限は必ずしも前述の実施例で説明したようにハードディスクユニット単位に設定する必要はなく、例えば、１台のハードディスクユニットの記憶エリアを分割し、分割された記憶エリアごとに異なるアクセス制限を施す、といったアクセス制限の仕方も考えられる。

【００２６】本番用ユニットＡと待避用ユニットＢとは前述の実施例のように１：１に対応づけられていてもよいし、１：ｎに対応づけられていてもよい。

【００２７】ストレージは、ディスクアレイ装置である場合に限られず、磁気ディスクシステムや光磁気ディスク装置（共に充分な容量のキャッシュやバッファを備えたもの）などでもよい。

【００２８】バックアップ装置は、前述したＤＡＴテープドライブ以外に、例えば、カセットテープ、８ｍｍテープ、９トラック・オープン・テープ、３４９０／３４９０Ｅカートリッジ・テープ、ＤＬＴ／ＳＤＬＴテープ、ＡＩＴテープ、ＴＲＡＶＡＮミニカートリッジ・テープ、ＤＴＦカートリッジ・テープ、ＬＴＯカートリッジ・テープ、ＺＩＰ、ＣＤ－Ｒ、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、ＭＯ、フロッピー（登録商標）ディスクなどのメディアを用いるものであってもよい。

【００２９】また、一般にストレージに実装されるハードディスクユニット１１は、ＲＡＩＤを構成していることが多いが、本発明はＲＡＩＤを構成しているかどうか＊に関わらず適用することができる。

【００３０】キーは、前述の実施例のように暗号化と復号化の双方に同一のキーを設定してもよいし、暗号化キーと復号化キーとを別個に設定してもよい。なお、この場合、暗号化キーと復号化キーは、例えば、図５に示すような形態で管理テーブルに管理されることになる。

【００３１】また、以上の説明では秘密鍵方式を前提とするものであるが、公開鍵暗号化方式を採用することも考えられる。

【００３２】

【発明の効果】以上説明したように、本発明によれば、高いデータセキュリティを確保しつつ、ストレージシステムにおけるストレージ内データのバックアップ管理を行うことが可能である。

【図面の簡単な説明】

【図１】本発明の一実施例による、データセンタに設置されたストレージシステムの概略構成を示す図である。

【図２】本発明の一実施例によるディスクアレイ装置の概略構成を示す図である。

【図３】本発明の一実施例による管理テーブルの一例を示す図である。

【図４】本発明の一実施例による、本番用ユニットのデータの復旧処理を説明するフローチャートである。

【図５】本発明の一実施例による管理テーブルの一例を示す図である。

【図６】従来のデータセンタにおけるストレージシステムの概略構成を示す図である。

【符号の説明】

１０　ディスクアレイ装置
１１　ハードディスクユニット
２０ａ，２０ｂ，２０ｃ　サーバ装置
３０　バックアップ装置（ＤＡＴテープドライブ）
５０　ＳＡＮ

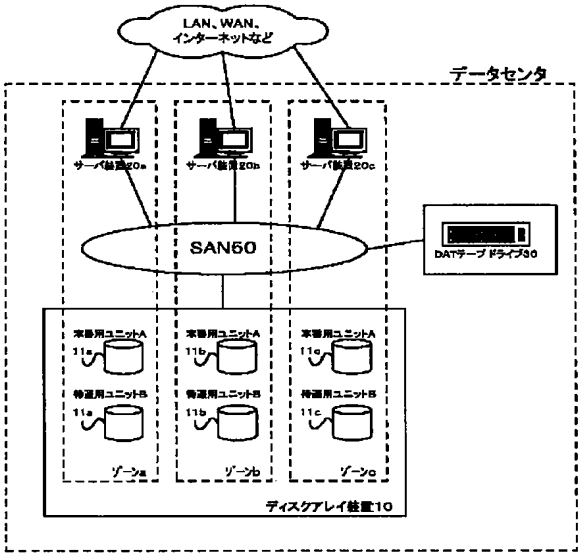
【図３】

本番用ディスクのユニットID	待避用ディスクのユニットID	暗号化キー
500	600	xxxyyyzzz
114	116	xxxzzzyyy
118	120	wwwssskkk
・	・	・
・	・	・
・	・	・
・	・	・
・	・	・

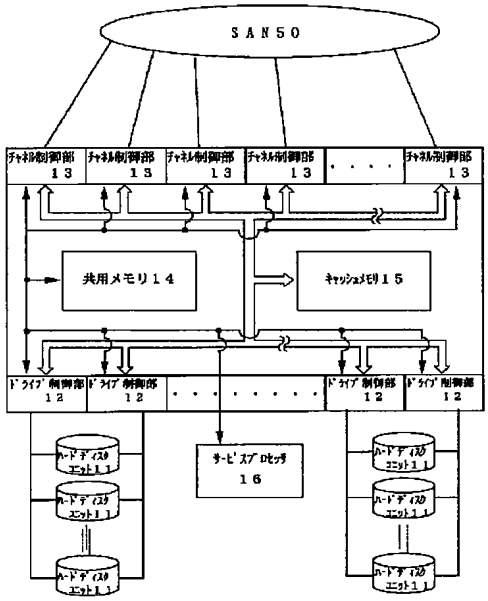
【図５】

本番用ディスクのユニットID	待避用ディスクのユニットID	暗号化キー	復号化キー
500	600	xxxyyyzzz	ssskkkjjj
114	116	xxxzzzyyy	pppqqquuu
118	120	wwwssskkk	yyyrrrlll
・	・	・	・
・	・	・	・
・	・	・	・
・	・	・	・
・	・	・	・

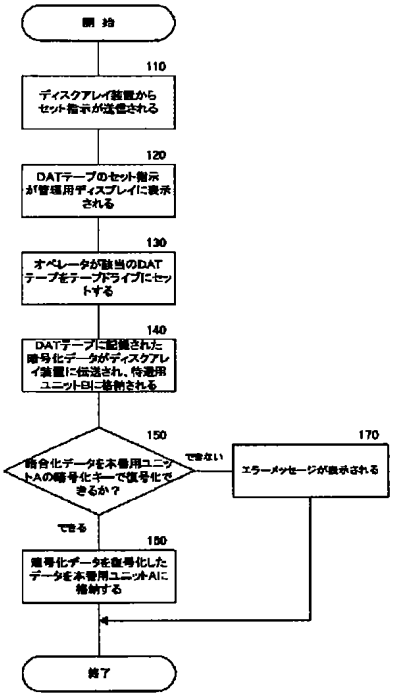
【図１】


LAN、WAN、
インターネットなど
データセンタ
SAN50
DATテープ ドライブ30
ディスクアレイ装置10

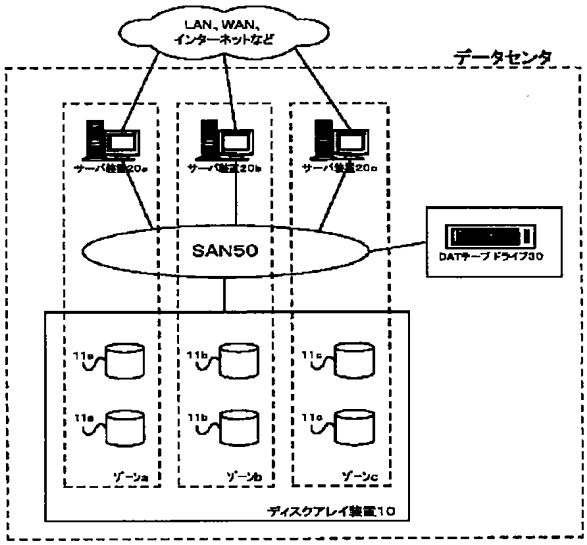
【図２】


SAN50
共用メモリ１４
キャッシュメモリ１５
サービスプロセッサ
１６

【図４】


開始
110
ディスクアレイ装置からセット指示が送信される
120
DATテープのセット指示が管理用ディスプレイに表示される
130
オペレータが該当のDATテープをテープドライブにセットする
140
DATテープに記録された暗号化データがディスクアレイ装置に転送され、待避用ユニットBに格納される
150
暗号化データを本番用ユニットAの暗号化キーで復号化できるか？
できない
170
エラーメッセージが表示される
できる
160
暗号化データを復号化したデータを本番用ユニットAに格納する
終了

【図６】


LAN、WAN、
インターネットなど
データセンタ
SAN50
DATテープ ドライブ30
ディスクアレイ装置10

フロントページの続き

Ｆターム(参考)　5B017 AA03 BA07 CA07
5B018 GA04 GA10 HA04 KA03 MA12
5B065 BA01 BA07 CA19 CE22 EA12
EA35 PA16 ZA15
5B082 DE04 DE07 GA11 HA05